REMARKS

Claims 1-16 are pending. In the Office Action of March 9, 2009, claims 1-14 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Mullen et al. (US 2003/0140141 A1) ("Mullen") in view of Kakivaya et al. (US 2004/0267876 A1) ("Kakivaya"). Claim 15 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Mullen in view of Kakivaya and further in view of official notice. The Applicants respectfully traverse the rejections and request reconsideration in view of the following remarks.

I. REJECTIONS UNDER 35 U.S.C. § 103(a)

Claims 1-14 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Mullen in view of Kakivaya. With this response, claims 1, 12 and 16 have been amended for clarity and not for reasons relating to patentability. No new matter has been added.

Independent claims 1, 12 and 16, as amended, and claim 7 are set forth above.

Mullen discloses "[s]ystems and methods for enabling universal remote access and display of diagnostic images acquired by diagnostic imaging equipment, independent of the identity of the vendor that manufactured the equipment. One system includes a local area network; a scanner capable of sending objects formatted in accordance with a communications protocol, each object incorporating at least one image frame; and a data capture device connected to the local area network and programmed with data capture software to capture an object originating from the scanner in response to that scanner being specified as an object of diagnosis. This system further includes a communications channel, e.g., a virtual private network, for connecting the data capture device to a central service facility. The preferred communications protocol is DICOM. In response to an instruction from the service center, the data capture device on the LAN captures image files from a malfunctioning scanner and forwards them to the service center for diagnosis" *See* Mullen, Abstract.

Kakivaya discloses "[a]n ad-hoc discovery protocol [which] improves reliability, security and scalability of multicast and server-based discovery. In switching from multicast to server-based discovery, the discovery client is made responsible for multicast suppression, and not discoverable devices with services. Messages include message identifier and time-to-live parameters to detect recast queries and avoid duplicating replies. A device's announcement message includes endpoint identifier, configuration number and stateless boot time parameters to detect changed device configuration and rebooted state for refreshing cached device and service descriptions. Paging parameters allow a discovery client to control the number of discovery responses returned at a time from a discovery server." *See* Kakivaya, Abstract.

Both Mullen and Kakivaya fail to disclose at least "identifying, automatically by a first device of said plurality of diagnostic medical imaging devices, a second device of said plurality of diagnostic medical imaging devices available for communication via said network based on an unsolicited identification message received by the first device from the second device; configuring, automatically, said first device to communicate substantially directly with said second device via said network when said first device is not already configured to communicate with said second device" as claimed in claim 1; "identification logic operative to periodically identify, via said network, said first diagnostic medical imaging device to other diagnostic medical imaging devices coupled with said network and receive a response therefrom, said identification logic being further operative to recognize other diagnostic medical imaging devices which identify themselves to said first diagnostic medical imaging device; configuration logic coupled with said identification logic and operative to automatically configure said first diagnostic medical imaging device to communicate with said other diagnostic medical imaging devices which at least one of respond and identify themselves when said first diagnostic medical imaging device is not already configured to communicate with said other diagnostic medical imaging devices which at least one of respond and identify themselves" as claimed in claim 7; "each of said plurality of diagnostic medical imaging devices being operative to automatically discover at least one other of said plurality of diagnostic medical imaging devices via said network based on unsolicited identification messages received over said network from the at least one other

of said plurality of diagnostic medical imaging devices, automatically configure itself to communicate with any of the discovered at least one other of said plurality of diagnostic medical imaging devices, and facilitate communications therebetween" as claimed in claim 12; or "wherein each of said plurality of diagnostic medical imaging devices comprises means for automatically discovering at least one other of said plurality of diagnostic medical imaging devices via said network based on unsolicited identification messages received over said network from the at least one other of said plurality of diagnostic medical imaging devices, automatically configuring itself to communicate with any of the discovered at least one other of said plurality of diagnostic medical imaging devices, and facilitating communications therebetween" as claimed in claim 16.

Mullen discloses instead:

> In addition to storing images internally, modern imaging systems need to be able to transfer images to various types of remote devices via a communications network. To successfully transfer images, *the relevant networking features of the scanner must be compatible with the networking features of the destination remote device*. *See* Mullen, para. 5 (emphasis added).
>
> In order to accomplish image transfer, the imaging system must know the configuration of the destination remote device prior to attempting to communicate with that device. *The configuration data for the destination remote device is typically inputted to the scanner during software installation by a field engineer*, although the DICOM network can be configured at any time. When the scanner receives an instruction to transmit data to a particular remote device from the system operator, the scanner software converts the image data to be transferred into the DICOM format required by the destination remote device, based on the configuration data for that device stored in the imaging system memory. The scanner also sends a request over the network to the destination remote device to open an association, i.e., to connect the scanner to the destination remote device. If the remote device responds in the affirmative, the scanner and remote device then agree on which device will act as the server and which as the client. The scanner also selects the appropriate encoding syntax from those accepted by the remote device. Other communication parameters are also negotiated. *See* Mullen, para. 7 (emphasis added).
>
> The scanner shown in FIG. 1 is designed to communicate with a configured remote device *only if that device has been "activated". Activation causes the DICOM presets manager 30 to configure one of a multiplicity of DICOM tasks 40 in accordance with configuration data entered into the system for the associated remote device*. That particular DICOM task will thereafter remain configured for that type of remote

> device until reconfigured for a different device. Other DICOM tasks are configured for other remote devices. *See* Mullen, para. 28 (emphasis added).
>
> In particular, a scanner can be configured to communicate with a DICOM-compatible computerized data capture device 52 connected to LAN 50. The data capture device 52 has a DICOM interface 54 that enables it to send and receive DICOM objects to and from the LAN 50. *See* Mullen, para. 34.

In particular, as shown by the excerpts above, Mullen merely discloses known manual configuration techniques for DICOM-compatible devices. Further, as Mullen is focused on sniffing or otherwise intercepting DICOM network communications for the purpose of diagnosing device failures, device-to-device configuration is largely ignored.

As in the prior office actions of May 12 and October 15, 2008, the Examiner, without specificity, argues that the following paragraph of Mullen discloses elements of Applicants' claims:

> The web server 76 may transmit and receive data to and from the scanners 64 via the network 74, and to and from the central service facility 66 through a firewall 78, particularly with a Point-to-Point Protocol (PPP). Firewall 78 may include any of various known security devices for preventing access to central service facility 66 except by recognized subscribers and other users. Central service facility 66 includes one or more central computers 68 which coordinate data exchange between the scanners 64 and service support workstations 70 at the central service facility. Workstations 70 may, in turn, be staffed by service personnel. Computer 68 may also be coupled for data exchange with one or more servers 72 at the central service facility. Moreover, computer 68 or other devices at the central service facility 66 may be coupled or configured to be coupled to other internal or external networks, such as for exchanging data with database 82 through an additional firewall 80. In the presently preferred configuration, database 82 may be local to or remote from the central service facility 66, and may contain data relating to the service history of particular scanners, families of scanners, and the like. Such data is compiled over time by transmission from computer 68, and is subsequently accessible by computer 68. *See* Mullen, para. 43.

However, contrary to the Examiner's assertions, the above excerpt generally describes the logical arrangement of devices in the disclosed network but fails to disclose any methodologies by which devices may be configured to communicate with other devices over a network as claimed. Accordingly, should the Examiner maintain his rejections, he is

respectfully requested to specifically point out how he is applying the above disclosure to show each element of Applicants' claims.

Kakivaya discloses instead that:

> … [t]he ad-hoc service discovery protocol generally involves 3 kinds of actors on a network: discovery clients (e.g., a controller, or like device seeking to discover services to control on the network), discovery responders (e.g., devices and services on devices, but possibly also controllers), and optionally a discovery server. *See* Kakivaya, para. 4.
>
> …
>
> In one implementation, the ad-hoc service discovery protocol described herein provides transport-neutral mechanisms to locate devices and services. The ad-hoc service discovery protocol involves exchanges of four basic message types between discovery clients, discovery responders and discovery servers, including: find, find response, announce, and bye-bye.
>
> The ad-hoc service discovery protocol can operate in two modes: either by sending a query (a find request message) to a multicast group, or by sending a query directly to a selected discovery server. In multicast mode, the devices whose device or service description matches the query return a response (a find response message) directly to the sender; in direct mode, the server provides a list of devices or services matching the query. The procedure by which clients discover servers and switch from multicast to server-based operation is called "multicast suppression." *See* Kakivaya, paras. 39-40.
>
> …
>
> The purpose of the ad-hoc service discovery protocol is to let discovery clients discover services hosted by devices. The data model is thus device centric: a device hosts services, or possibly other devices; the find responses will carry a description of the device and of all the hosted services. *See* Kakivaya, para. 64.

As can be seen from the above excerpts, Kakivaya discloses a system where by devices broadcast queries, or otherwise queries a server, looking to see if particular devices matching the query exist on the network. If matching devices exist, they respond, or the server responds with a list of matching devices. However, in contrast to Applicants claims, the devices of Kakivaya do not listen for unsolicited identification messages and then configure themselves to communicate with the senders of those unsolicited messages as

claimed. The Kakivaya devices, instead, actively solicit the identity of devices that meet the desired criteria rather than waiting for those devices to identify themselves.

Further, one of ordinary skill in the art would not be motivated to modify the protocol of Kakivaya as it would defeat the stated purpose "....of the ad-hoc service discovery protocol ...to let discovery clients discover services hosted by devices." *See* Kakivaya, para. 64.

For at least these reasons, claims 1, 7, 12 and 16 are patentable over Mullen and Kakivaya, alone or in combination. Applicants therefore request that the Examiner withdraw this rejection of these claims.

Claims 2-6, 8-11 and 13-14 depend from claims 1, 7 and 12 and are therefore allowable for at least the reasons set forth above. Accordingly, Applicants request that the Examiner withdraw the rejections of claims 2-6, 8-11 and 13-14.

Claim 15 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Mullen in view of Kakivaya and further in view of official notice. Claim 15 depends from claim 12 and is therefore allowable for the reasons set forth above with regard to this claim. Accordingly, Applicants request that the Examiner withdraw this rejection of claim 15.

CONCLUSION

Applicants submit that all of the pending claims are in condition for allowance and notice to this effect is respectfully requested.

PLEASE MAIL CORRESPONDENCE TO:

Siemens Corporation
Customer No. 28524
Attn: Elsa Keller, Legal Administrator
170 Wood Avenue South
Iselin, NJ 08830

Respectfully submitted:

/Rosa S. Kim/

Rosa S. Kim, Reg. No. 39,728
Attorney(s) for Applicant(s)
650-694-5330
Date: June 2, 2009